PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347808
(43)Date of publication of application : 15.12.2000

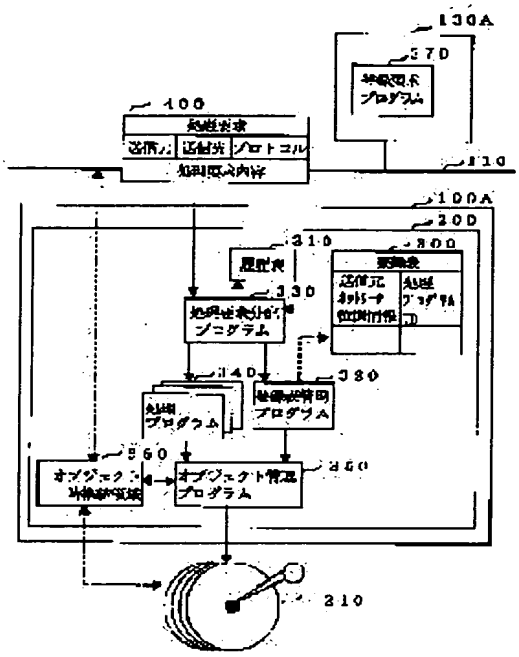
(51)Int.Cl. G06F 3/06
G06F 12/14
G06F 13/00

(21)Application number : 11-154646
(22)Date of filing : 02.06.1999

(71)Applicant : HITACHI LTD
(72)Inventor : TOMITA AKI
ODAWARA HIROAKI

(54) DISK DEVICE DIRECTLY CONNECTABLE TO NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To guarantee the security of a magnetic disk device directly connectable to a network by providing a means for discriminating whether a data processing request can be executed or not corresponding to the transmission source of a packet when the packet containing that data processing request is received.
SOLUTION: A computer investigates whether or not a computer is registered on a registration table 300 and the protocol of requested processing is permitted or not. When it is registered and the protocol is permitted, a processing program 340 corresponding to the requested protocol is run. When it is not registered or the protocol is not registered, processing request contents are recorded on a history table 310 and processing is finished. In this case, error contents are not returned to the processing request transmission source of a magnetic disk device 100A. Thus, the computer, which is not registered in the magnetic disk device 100A or whose protocol is not processed yet, can not know the existence of the magnetic disk device 100A.



LEGAL STATUS

[Date of request for examination] 18.03.2003
[Date of sending the examiner's decision of rejection] 13.06.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－347808
(P2000－347808A)
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	3/06	301	G06F	3/06	301A　5B017
		304			304H　5B065
	12/14	310		12/14	310K　5B089
	13/00	357		13/00	357A

審査請求　未請求　請求項の数6　ＯＬ　（全 5 頁）

(21)出願番号　特願平11－154646

(22)出願日　平成11年6月2日(1999.6.2)

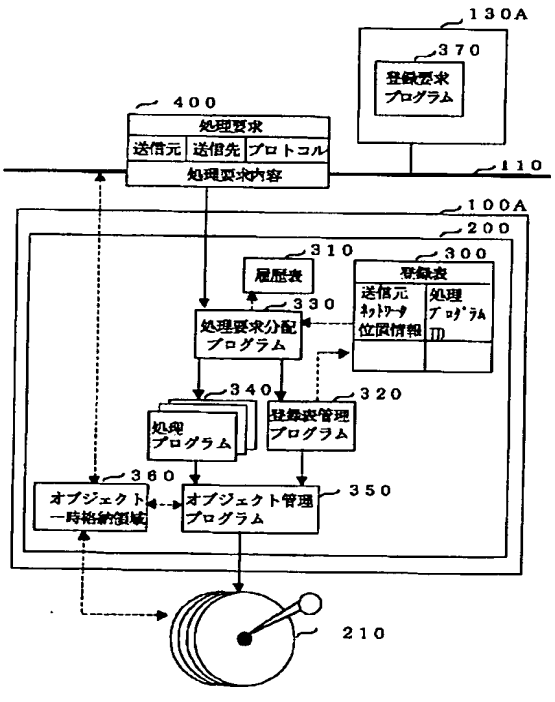
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(72)発明者　富田　亜紀
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　小田原　宏明
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ネットワークに直接接続可能なディスク装置

(57)【要約】
【課題】　ネットワークに直接接続可能な磁気ディスク装置のセキュリティを保証することにある。
【解決手段】　磁気ディスク装置を使用可能な計算機のネットワーク上の位置情報とその計算機に許可するプロトコルを磁気ディスク装置に登録する。また、磁気ディスク装置に、受け取った処理要求が許可されているか否かを判定する機能や、許可されていない場合には履歴をとる機能を付加する。
【効果】　磁気ディスク装置へのアクセスを制限して磁気ディスク装置のセキュリティを向上させることができる。

図3



【特許請求の範囲】
【請求項１】プログラムを実行可能なプロセッサと、
データを記憶するための記憶媒体と、
ネットワークへの接続機構と、
上記ネットワークを介してデータ処理要求を含むパケットを受信した場合、そのパケットの送信元に応じてそのデータ処理要求が実行可能か否かを判定する手段とを有することを特徴とするネットワークに直接接続可能なディスク装置。
【請求項２】上記データ処理要求が要求する処理プロトコルに応じて、そのデータ処理要求が実行可能か否かを判定することを特徴とする請求項１に記載のネットワークに直接接続可能なディスク装置。
【請求項３】複数の処理プロトコルを処理する手段を有することを特徴とする請求項２に記載のネットワークに直接接続可能なディスク装置。
【請求項４】プログラムを実行可能なプロセッサと、
データを記憶するための記憶媒体と、
ネットワークへの接続機構と、
上記ネットワークに接続された計算機のネットワークアドレスと、上記計算機が処理要求することができる処理プロトコルとを記憶手段に登録する手段と、
上記ネットワークを介してデータ処理要求を受信した場合，そのデータ処理要求が上記登録された計算機であるか否かを判定する手段とを有することを特徴とするネットワークに直接接続可能なディスク装置。
【請求項５】上記データ処理要求が上記登録された処理プロトコルであるか否かを判定する手段を有することを特徴とする請求項４に記載のネットワークに直接接続可能なディスク装置。
【請求項６】上記記憶手段に登録するためのプロトコルを複数有することを特徴とする請求項４又は請求項５の何れかに記載のネットワークに直接接続可能なディスク装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークに直接接続可能な磁気ディスク装置のアクセス制御方式に関する。
【０００２】
【従来の技術】従来、磁気ディスク装置は、そのハードウェア制約のため、一定のブロックサイズに基づいてデータを管理し、Ｐｏｉｎｔ－ｔｏ－Ｐｏｉｎｔ通信方式によりデータを転送する、といった簡単な機能しか提供していなかった。
【０００３】ＡＮＳＩ（Ａｍｅｒｉｃａｎ　Ｎａｔｉｏｎａｌ　Ｓｔａｎｄａｒｄ　Ｉｎｓｔｉｔｕｉｔｅ）が開発し、磁気ディスク装置と計算機間のインタフェースとして広く使用されているＳＣＳＩ（Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）においては、ファイルやテーブルといった論理的に一塊のデータの単位ではなく、ブロック単位によりチャネル上でデータ入出力を行う。ＳＣＳＩは低位なインタフェースしか提供しないので、ファイルやテーブルといった論理的な高位のインタフェースを実現するためには、磁気ディスク装置が直接接続される計算機上でファイルシステムやデータベース管理システムが実行されていた。
【０００４】近年、ハードウェア技術の進歩と低価格化を背景として、ネットワークに接続するための機構を備え、磁気ディスク装置とデータ入出力を要求する計算機間に他の計算機を介さず直接データ入出力を行うことができるＮＡＳＤ（Ｎｅｔｗｏｒｋ－Ａｔｔａｃｈｅｄ　Ｓｅｃｕｒｅ　Ｄｉｓｋ）がカーネギーメロン大学のＧ．Ｇｉｂｓｏｎにより提案された（Ｔｈｅ　８ｔｈ　ＡＳＰＬＯＳ　Ｃｏｎｆｅｒｅｎｃｅ予稿集、１９９８年）。ＮＡＳＤはネットワーク接続機構を備えているだけではなく、ファイルといった論理的に一塊のデータ単位に基づいてデータを管理する。
【０００５】ＮＡＳＤでは、磁気ディスク装置とデータ入出力を要求する計算機間に他の計算機を介さず直接データ入出力を行うことができるので、悪質な第三者がＮＡＳＤに不正アクセスすることが可能である。そのため、ＮＡＳＤでは、高いセキュリティを保証するために、暗号化技術を用いたプロトコルを提供している。
【０００６】
【発明が解決しようとする課題】ＮＡＳＤへの処理要求のセキュリティは、ＮＡＳＤプロトコルが実装されている通信階層において検証される。現在、ＮＡＳＤプロトコルはＲＰＣ（Remote Procedure Call）上に実装されている。ＲＰＣは、一般には、ＯＳＩ（Open Systems Interconnection）のトランスポート層に相当するＵＤＰやＴＣＰ上に実装される。つまり、ＮＡＳＤへの処理要求のセキュリティはトランスポート階層よりも下位の、例えば、ＩＰといったネットワーク層においては検証されない。たとえ、ＮＡＳＤのセキュリティ機構が処理要求は不法侵入か否かを検証するとしても、何度でもＮＡＳＤのセキュリティ機構を破ろうと試みることが可能であり、不法な処理要求はＮＡＳＤプロトコルが実装されているネットワーク層以下の階層には到達している。
【０００７】一般に、ネットワークに接続されている計算機には、例えば、ＮＦＳ（Ｎｅｔｗｏｒｋ　Ｆｉｌｅ　Ｓｙｓｔｅｍ）といった分散ファイルシステムやＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）といった管理サービスなどの複数のサービスプロトコルが登録されている。実際には、ネットワーク直接接続型ディスク装置も、ＮＡＳＤプロトコルだけといったように一つのサービスプロトコルだけではなく、複数のサービスプロトコルを提供可能であるように実装する可能性が高い。この場合、ＮＡＳＤプロトコル以外のサービスプロトコルのセキュリティ

が低いと、ディスク装置のセキュリティは保証されない。

【０００８】そこで、本発明は、ネットワークに直接接続可能な磁気ディスク装置のセキュリティを保証することにある。

【０００９】

【課題を解決するための手段】上記の課題を達成するために、本発明の磁気ディスク装置は、受け取った処理要求を該当するサービスプロトコルの処理部に処理要求を渡す前に、不法侵入か否かを判定するプログラムを実行する。磁気ディスク装置は処理要求の発行を許可している計算機のネットワーク上の位置情報を登録している。判定プログラムは登録されていないネットワーク上の位置を送信元とする処理要求であることを判定すると、不法侵入と見なして棄却し、その処理要求の記録をとる。

【００１０】

【発明の実施の形態】本発明によるネットワークに直接接続された磁気ディスク装置のアクセス制御方式の一実施例を図面を用いて説明する。

【００１１】［１］構成の概略

図１は、本発明の磁気ディスク装置を用いたシステムのハードウェア構成例を示している。磁気ディスク装置１００Ａ、１００Ｂ、１００Ｃや計算機や磁気ディスク装置であるオブジェクト管理設定要求実体１３０Ａ、１３０Ｂはネットワーク１１０で接続されている。磁気ディスク装置は、ファイルやテーブル、レコードといった論理的なデータ単位であるオブジェクト１２０Ａ、１２０Ｂ、１２０Ｃを格納している。

【００１２】図２は個々の磁気ディスク装置のハードウェア構成を示している。各磁気ディスク装置は、電源によりバックアップされているメモリ２００、磁気ディスク媒体２１０、一つもしくは複数個のプロセッサ２２０を持つ。

【００１３】図３は本発明の一実施例の構成を示している。磁気ディスク装置１００Ａは登録表３００、履歴表３１０や登録表管理プログラム３２０、処理要求分配プログラム３３０、処理プログラム３４０、オブジェクト管理プログラム３５０をメモリ２００に置いて実行する。登録表３００は、磁気ディスク装置１００Ａを使用可能な計算機のネットワーク上の位置情報とその計算機に許可されている処理プロトコルの対を保持している。処理プロトコルの例としては、ＮＡＳＤプロトコルやＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）、ＪＭＡＰＩ（Ｊａｖａ　Ｍａｎａｇｅｍｅｎｔ　ＡＰＩ）が挙げられる。登録表管理プログラム３２０は、磁気ディスク装置１００Ａの電源を入れると磁気媒体２１０から読み出されて実行される。磁気ディスク装置１００Ａを管理する計算機１３０Ａは磁気ディスク装置１００Ａを使用可能な計算機を登録するための登録要求プログラム３７０を保持する。

【００１４】登録要求プログラム３７０を計算機１３０Ａ上で手動でインストールして動作させることもできる。また、計算機１３０Ａ上からＷＥＢブラウザのようなネットワークアクセスプログラムを介して、磁気ディスク装置１００Ａから登録要求プログラム３７０を計算機１３０Ａ上にダウンロードして動作させることもできる。さらに、登録要求プログラム３７０が動作する計算機１３０Ａは登録表管理プログラム３２０が動作する磁気ディスク装置１００Ａと等しい場合もある。つまり、登録表管理プログラム３２０と登録要求プログラム３７０は同じ磁気ディスク装置１００Ａ上で動作させることもできる。磁気ディスク装置１００Ａの電源を入れて登録表管理プログラム３２０を磁気ディスク媒体２１０から読み出して実行すると、登録表管理プログラム３２０は、ディスプレイなどの表示装置に登録要求プログラム３７０を磁気ディスク装置１００Ａにおいて実行するか否か、という質問を表示する。磁気ディスク装置１００Ａにおいて実行するように指定された場合には登録要求プログラム３７０は磁気ディスク装置１００Ａ上で動作する。

【００１５】磁気ディスク装置１００Ａは磁気ディスク装置１００Ａを使用可能な計算機を登録する際のプロトコルを複数保持することが可能である。磁気ディスク装置１００Ａを管理する計算機１００Ａは、登録に必要なセキュリティに応じて登録プロトコルを選択し、登録要求プロトコル３７０を介して選択したプロトコルに従って登録表管理プログラム３２０とやりとりして磁気ディスク装置１００Ａを使用可能な計算機を登録する。登録プロトコルの例としては、電子認証方式を用いたり、パスワードを用いたりするプロトコルが挙げられる。

【００１６】オブジェクト管理プログラム３５０は処理プログラム３４０が発行する磁気ディスク媒体２１０上に格納されているオブジェクトの入出力要求を処理する。オブジェクト管理プログラム３５０は、磁気ディスク媒体２１０に書き込むオブジェクトや磁気ディスク媒体２１０から読み出したオブジェクトを一時的にオブジェクト一時格納領域３６０に格納する。

【００１７】処理要求４００は、計算機から磁気ディスク装置１００Ａに送信される処理要求の形式を示している。処理要求４００は、送信元のネットワーク上の位置情報、送信先のネットワーク上の位置情報、プロトコルの種類等を保持する。ネットワーク上の位置情報の例としては、ＩＰアドレスとポート番号の対が挙げられる。

【００１８】本実施例では、磁気ディスク装置１００Ａを使用可能な計算機として計算機１３０Ｂが登録されている場合を想定する。図４は処理要求分配プログラム３３０の処理の流れを示している。まず、計算機１３０Ｂが登録表３００に登録されており、要求する処理のプロトコルが許可されているか否かを調べる（ステップ５０

０）。登録されており、かつ、プロトコルが許可されている場合には、要求するプロトコルに該当する処理プログラム３４０を実行する（ステップ５１０）。登録されていない、あるいは、プロトコルが許可されていない場合には、履歴表３１０に処理要求内容を記録して（ステップ５２０）終了する。この場合、磁気ディスク装置１００Ａ処理要求送信元にエラー内容を返さない。このことにより、磁気ディスク装置１００Ａに登録されていない、あるいは、プロトコルが処理されていない計算機は磁気ディスク装置１００Ａが存在したことも知ることができない。

【００１９】

【発明の効果】本発明によれば、ネットワークに直接接続可能な磁気ディスク装置へのアクセスを制限することにより、当該装置のセキュリティを保証することができる。

【図面の簡単な説明】

【図１】本発明の磁気ディスク装置の一実施例を示す図。

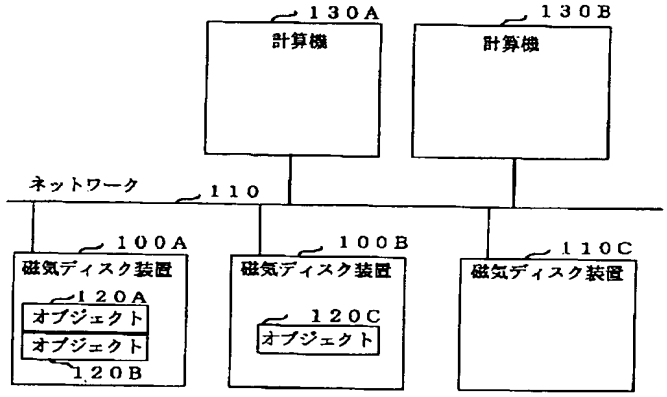
【図２】本発明の磁気ディスク装置のハードウェア構成を示す図。

【図３】本発明の磁気ディスク装置に実装されるソフトウェア構成を示す図。

【図４】磁気ディスク装置の処理要求分配プログラムのフローチャートを示す図。

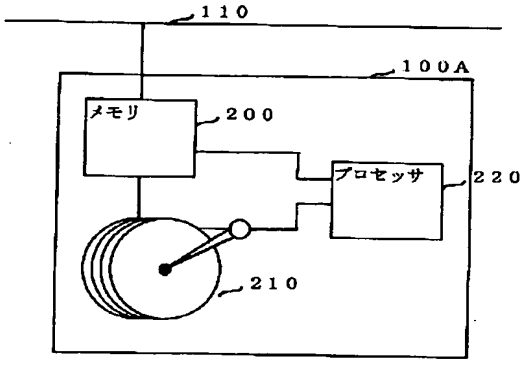
【図１】

図１



【図２】

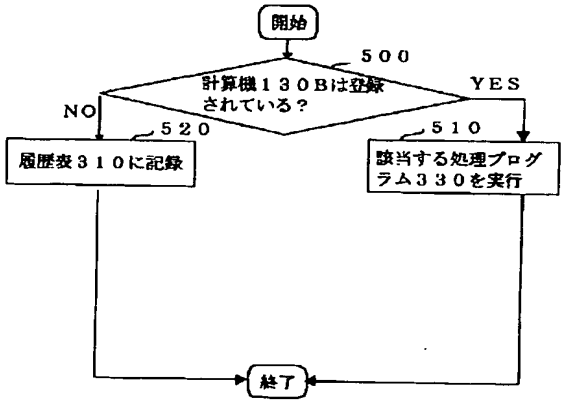
図２



【図４】

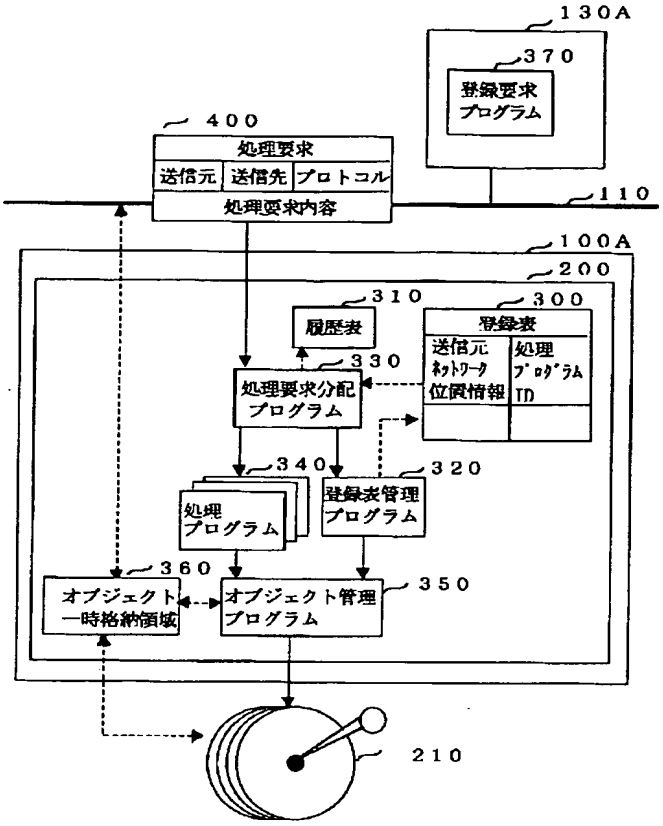
図４

３３０　処理要求分配プログラム



【図３】

図３



フロントページの続き

Ｆターム(参考) 5B017 AA01 BA05 BA06 BA09 BB10
CA06 CA07 CA16
5B065 BA01 CA01 CE01 PA13 PA14
5B089 GA12 JA35 KA17 KB13